UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,227	09/27/2001	Jeffrey Scott Bardsley	RSW920010166US1	5924

7590	09/14/2006	EXAMINER

Jack Friedman
SCHMEISER OLSEN and WATTS
3 Lear Jet Lane
Suite 201
Lathan, NY 12110

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
	09/966,227	BARDSLEY ET AL.
Office Action Summary	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 July 2006</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>5-7,10-12 and 19-30</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>5-7,10-12 and 19-30</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>27 November 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

1   This action is in response to the communication filed on 7/05/2006.

2   **DETAILED ACTION**

3   *Response to Arguments*

4   Applicant's arguments filed 7/5/2006 have been fully considered but they are not

5   persuasive.

6   Regarding applicants' argument that Sharma does not teach performing the determining

7   and comparing steps **whenever** the step of generating an alert is performed, the examiner does

8   not find the argument persuasive. The examiner notes that the claims do not recite "whenever",

9   but rather they recite "when". As such, the examiner notes that if the prior art teaches that one

10   time, when generating an alert the determining and comparing is performed, then the claims are

11   anticipated. The applicants are relying on Col. 9 Lines 16-20 of Sharma as showing that for the

12   first 999 alerts the determining and comparing is not performed when generating the alert, and

13   thus the claims are not anticipated. If we look at Col. 9 Lines 21-26 of Sharma, it is clearly seen

14   that from alert 1000 and beyond the determining and comparing is performed and thus the claim

15   limitations are taught by Sharma. Again, the examiner notes that the claim language does not

16   require that every time an alert is generated the steps are performed, but instead only requires

17   that the steps are performed for one alert generation.

18   Regarding applicants' argument that Sharma did not teach "altering an element of a

19   signature set of the [IDS]" in order to decrease the alert generation rate, the examiner does not

20   find the argument persuasive. Sharma teaches that, in one embodiment, in order to decrease the

21   alert generation rate, the network element is commanded to suspend generation of threshold

22   crossing alerts for a period of time, as seen in Col. 7 Paragraph 1 of Sharma. This meets the

1   limitation of the claim. Col. 9 Line 54 – Col. 10 Line 11 further teaches lowing the alert

2   generation rate by commanding the network element that is generating the most alerts of a

3   particular type to stop generating that particular alert for a given period of time. This too meets

4   the limitation of the claim. As such, the prior art clearly teaches the claimed feature and thus the

5   examiner does not find the argument persuasive. If the applicants' still believe that the feature is

6   missing in the cited references, the examiner encourages the applicants' to particularly point out

7   what is missing and why it is missing.

8   Claims 5-7, 10-12, and 19-30 have been examined, while claims .

9   All objections and rejections not set forth below have been withdrawn.

10   *Claim Rejections - 35 USC § 103*

11   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

12   obviousness rejections set forth in this Office action:

13   *A patent may not be obtained though the invention is not identically disclosed or*
14   *described as set forth in section 102 of this title, if the differences between the subject matter*
15   *sought to be patented and the prior art are such that the subject matter as a whole would have*
16   *been obvious at the time the invention was made to a person having ordinary skill in the art to*
17   *which said subject matter pertains. Patentability shall not be negatived by the manner in which*
18   *the invention was made.*
19

20   Claims 5, 10, and 19-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over

21   Vaidya (US Patent Number 6,279,113), and further in view of Sharma et al. (US Patent Number

22   6,909,692) hereinafter referred to as Sharma

23   Regarding claim 5, Vaidya disclosed a method of operating an intrusion detection system,

24   comprising the steps of: monitoring, by the intrusion detection system, for occurrence of a

25   signature event that is indicative of a DOS intrusion on a protected device, said DOS attack

1   attempting to impede operation of the protected device (See Vaidya Abstract and Col. 12

2   Paragraphs 2-3); when a signature event occurs, increasing a value of a signature event counter

3   and comparing the value of the signature event counter with a signature threshold quantity (See

4   Vaidya Col. 12 Lines 26-36); when the value of the signature event counter exceeds the signature

5   threshold quantity, generating an alert by the intrusion detection sensor of the intrusion detection

6   system (See Vaidya Col. 12 Lines 36-41, Col. 11 Lines 5-8, and Col. 6 Lines 20-26); but Vaidya

7   failed to disclose recording a time for generating the alert in a log of a governor comprised by the

8   intrusion detection sensor, determining from the contents of the log a present alert generation

9   rate, and comparing the present alert generation rate with an alert generation rate threshold; or

10   when the present alert generation rate exceeds the alert generation rate threshold, altering an

11   element of a signature set of the intrusion detection system to decrease an alert generation rate of

12   the intrusion detection system.

13   Sharma teaches that generating too many alerts in a network management system can

14   crash the system (See Sharma Col. 3 Paragraph 3) and further teaches that in order to control the

15   alert generation rate, each alert should be logged including a time of the alert (See Sharma Col. 8

16   Line 61 – Col. 9 Line 15), an alert generation rate should be determined using the log (See

17   Sharma Col. 9 Lines 16-25), the determined rate should be compared with a threshold (See

18   Sharma Col. 9 Lines 25-27), and when the rate is too high, altering the management system to

19   decrease an alert generation rate of the system (See Sharma Col. 9 Line 28 – Col. 10 Line 15 and

20   Col. 7 Lines 1-23).

21   It would have been obvious to the ordinary person skilled in the art at the time of

22   invention to employ the teachings of Sharma in the IDS system of Vaidya by the reaction module

1   logging the alerts, determining the alert generation rate, comparing the rate to the threshold rate,

2   and if greater than the threshold altering the attack signature profile to indicate a new threshold

3   for event rate in order to begin transmitting alerts again. This would have been obvious because

4   the ordinary person skilled in the art would have been motivated to protect the system

5   administrator from being over informed as well as protecting the management system from

6   crashing.

7   Regarding claim 10, Vaidya disclosed programmable media containing programmable

8   software for operation of an intrusion detection system, programmable software comprising the

9   steps of: monitoring, by the intrusion detection system, for occurrence of a signature event that is

10   indicative of a DOS intrusion on a protected device, said DOS attack attempting to impede

11   operation of the protected device (See Vaidya Abstract and Col. 12 Paragraphs 2-3); when a

12   signature event occurs, increasing a value of a signature event counter and comparing the value

13   of the signature event counter with a signature threshold quantity (See Vaidya Col. 12 Lines 26-

14   36); when the value of the signature event counter exceeds the signature threshold quantity,

15   generating an alert by the intrusion detection sensor of the intrusion detection system (See

16   Vaidya Col. 12 Lines 36-41, Col. 11 Lines 5-8, and Col. 6 Lines 20-26); but Vaidya failed to

17   disclose recording a time for generating the alert in a log of a governor comprised by the

18   intrusion detection sensor, determining from the contents of the log a present alert generation

19   rate, and comparing the present alert generation rate with an alert generation rate threshold; or

20   when the present alert generation rate exceeds the alert generation rate threshold, altering an

21   element of a signature set of the intrusion detection system to decrease an alert generation rate of

22   the intrusion detection system.

1   Sharma teaches that generating too many alerts in a network management system can

2   crash the system (See Sharma Col. 3 Paragraph 3) and further teaches that in order to control the

3   alert generation rate, each alert should be logged including a time of the alert (See Sharma Col. 8

4   Line 61 – Col. 9 Line 15), an alert generation rate should be determined using the log (See

5   Sharma Col. 9 Lines 16-25), the determined rate should be compared with a threshold (See

6   Sharma Col. 9 Lines 25-27), and when the rate is too high, altering the management system to

7   decrease an alert generation rate of the system (See Sharma Col. 9 Line 28 – Col. 10 Line 15 and

8   Col. 7 Lines 1-23).

9   It would have been obvious to the ordinary person skilled in the art at the time of

10   invention to employ the teachings of Sharma in the IDS system of Vaidya by the reaction module

11   logging the alerts, determining the alert generation rate, comparing the rate to the threshold rate,

12   and if greater than the threshold altering the attack signature profile to indicate a new threshold

13   for event rate in order to begin transmitting alerts again. This would have been obvious because

14   the ordinary person skilled in the art would have been motivated to protect the system

15   administrator from being over informed as well as protecting the management system from

16   crashing.

17   Regarding claims 19 and 25, Vaidya and Sharma disclosed alerting an administrator of

18   suspected DOS intrusions upon the protected device (See Vaidya Col. 6 Lines 20-26).

19   Regarding claims 20 and 26, Vaidya and Sharma disclosed that the alert generation rate

20   threshold is comprised by the governor (See Sharma Col. 9 Lines 16-26).

21   Regarding claims 21 and 27, Vaidya and Sharma disclosed that the signature set

22   comprises a unique signature set identifier (See Vaidya Col. 10 Lines 25-45 "Pattern"), the

1   signature event (See Vaidya Col. 10 Lines 25-45 "Attack_Signature"), the signature event

2   counter (See Vaidya Col. 12 Paragraph 3 "counter"), the signature threshold quantity (See

3   Vaidya Col. 12 Paragraph 3 "threshold"), and a signature threshold interval that specifies a

4   sliding time window (See Vaidya Col. 12 Paragraph 3 "predetermined time interval".

5   Regarding claims 22 and 28, Vaidya and Sharma disclosed that the protected device is

6   selected from the group consisting of a computer, a web server, and a workstation (See Vaidya

7   Col. 10 Lines 54-57).

8   Regarding claims 23 and 29, Vaidya and Sharma disclosed entering into the log a list of

9   timestamps that record the times at which the intrusion detection sensor generates alerts, wherein

10   said determining from contents of the log a present alert generation rate utilizes the timestamps

11   in the log (See Sharma Col. 9 Paragraph 2).

12   Regarding claims 24 and 30, Vaidya and Sharma disclosed that after generating the alert

13   and before determining from contents of the log the present alert generation rate, the method

14   further comprises the step of: clearing the log of any entries that are past a specific age (See

15   Sharma Col. 9 Paragraph 2 and Vaidya Col. 12 Paragraph 2 wherein Vaidya disclosed purging

16   the expired entries of a log prior to determining the generation rate associated with the log).

17   Claims 6, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over the

18   combination of Vaidya and Sharma as applied to claims 5, and 10 above respectively, and further

19   in view of Lunt (Detecting Intruders in Computer Systems).

20   Vaidya and Sharma disclosed altering the signature set in order to reduce the frequency

21   of alert generation by halting the alert generation (See the rejection of claim 5 above), but failed

22   to disclose altering the threshold quantity in order to do so.

1   Lunt teaches that alarms do not always pertain to individual events, and because they can

2   come very quickly, after the first alarm is generated, subsequent alarms should be suppressed

3   until a second threshold, greater than the first, is reached (See Lunt Page 14 Lines 11-17).

4   It would have been obvious to the ordinary person skilled in the art at the time of

5   invention to employ the teachings of Lunt in the alert generation system of Vaidya and Sharma,

6   by suppressing alerts after the first threshold was reached, until a higher threshold is reached.

7   This would have been obvious because the ordinary person skilled in the art would have

8   recognized that multiple attacks can occur at the same time and would not want to ignore attacks

9   after the first initial attack.

10   Claims 7, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over the

11   combination of Vaidya and Sharma as applied to claims 5, and 10 above respectively, and further

12   in view of Martin et al. (US Patent Number 6,772,349) hereinafter referred to as Martin.

13   Vaidya and Sharma disclosed altering the signature set in order to reduce the frequency

14   of alert generation by halting the alert generation (See the rejection of claim 5 above) and that

15   the generation rate was determined using a sliding time window (See Vaidya Col. 12 Paragraph

16   2), but failed to disclose altering the threshold interval in order to do so.

17   Martin teaches that in a network intrusion detection system, the time interval used to

18   collect signature data is indirectly proportional to the number of false alarms detected (See

19   Martin Col. 5 Lines 30-38).

20   It would have been obvious to the ordinary person skilled in the art at the time of

21   invention to employ the teachings of Martin in the alert suppressing system of Vaidya and

22   Sharma, by decreasing the time interval once the threshold was broken. This would have been

1   obvious because the ordinary person skilled in the art would have been motivated to ensure that

2   legitimate alerts were detected while false alarms were reduced.

3

4   *Conclusion*

5   Claims 5-7, 10-12, and 19-30 have been rejected.

6   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

7   policy as set forth in 37 CFR 1.136(a).

8   A shortened statutory period for reply to this final action is set to expire THREE

9   MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

10 MONTHS of the mailing date of this final action and the advisory action is not mailed until after

11 the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

12 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

13 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

14 however, will the statutory period for reply expire later than SIX MONTHS from the mailing

15 date of this final action.

16

17   Any inquiry concerning this communication or earlier communications from the

18 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.

19 The examiner can normally be reached on M-F 8-4.

20   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

21 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

22 organization where this application or proceeding is assigned is 571-273-8300.

1   Information regarding the status of an application may be obtained from the Patent

2   Application Information Retrieval (PAIR) system. Status information for published applications

3   may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

4   applications is available through Private PAIR only. For more information about the PAIR

5   system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

6   system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

7
8
9
10
11   AYAZ SHEIKH
12   SUPERVISORY PATENT EXAMINER
13   TECHNOLOGY CENTER 2100
14   Matthew Henning
15   Assistant Examiner
16   Art Unit 2131
17   9/7/2006